フィッシングを教える際の手順、ポイント

手順

①にせフィッシングを体験する。

②教材を見ながらフィッシングに関する解説をする。

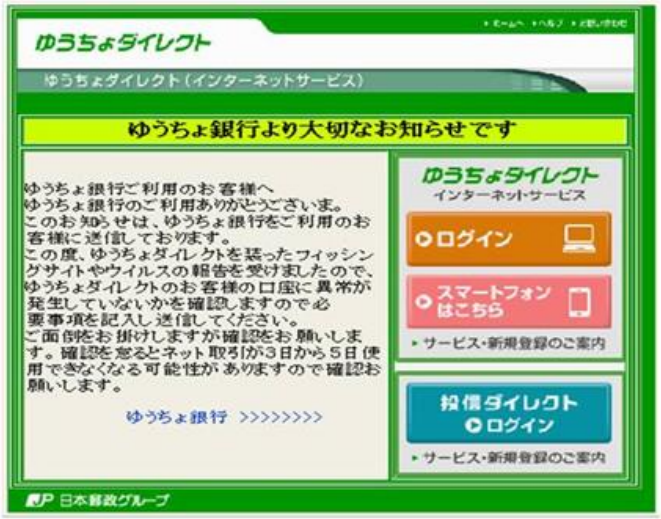
- フィッシングとは偽物のウェブサイトに誘導して銀行なら口座番号や暗証番号、ウェブサービスならメールアドレス、アカウント名、パスワードを盗み取ることを指す。
- フィッシングの手口は巧妙で偽物のウェブサイトはぱっと見では見分けがつかないこと。
- 本物のウェブサイトであってもポップアップで表示される入力画面はフィッシングである。

フィッシング

フィッシングは偽物の銀行やSNSなどのサイトに誘導して、口座番号やアカウント情報を盗むことネット犯罪です。

例えば銀行の場合、右のゆうちょ銀行のフィッシングサイトでは「ゆうちょダイレクトを装ったフィッシングサイトやウイルスサイトの報告を受けましたので口座に以上が発生していないか確認しています」と個人情報を入力するよう促しています。

また、昨今のフィッシングはとてもよくできており本物と偽物の見分けがつかないほどです。下２つは三菱東京UFJ銀行のフィッシングサイトと本物のサイトです。見た目だけで区別をつけることは不可能です。



偽物

本物

<u>どうしたらいいの？</u>

銀行以外にもFacebookやツイッターなどのSNSでもフィッシングサイトはあります。

フィッシングに対しては

① OS、アプリケーション、セキュリティソフトを最新のものにする。

② 銀行が電話やメールで暗証番号を確認することは絶対にないことを知っておく。

③ もし、不安になったらそのサイトの運営会社に連絡を取り確認する。

以上３つのことを心がけましょう。